IN THE SPECIFICATION:

Please replace paragraph 0036 (beginning at page 9) with the following rewritten paragraph:

--The copy of the authoritative record can be viewed, printed, and saved at, as well as retransmitted from, the remote location without compromising the integrity of the authoritative record at the repository. The method comprises receiving an electronic record in the repository, creating an authoritative electronic record of the received record by appending information to the end of the electronic record, digitally signing the electronic record and appended information to form a receipt, prepending this receipt information to the beginning of the electronic record, appending additional information to the end of the electronic record, and storing this whole as the authoritative electronic record in the repository. The authoritative electronic record is unique since no other exact representation of it exists anywhere else outside the repository. The concatenated whole of all information prepended to the beginning of the record is referred to as the beginning information. The concatenated whole of all information appended to the end of the electronic record is referred to as the ending information.--

Please replace paragraph 0037 (beginning at page 9) with the following rewritten paragraph:

--When a copy of the authoritative electronic record is requested by a person at a remote location, a copy is made by making a copy of the electronic record and the appended ending information only. The system then provides for transmitting a version of the copy to the person at the remote location, wherein transmission may be over the un-trusted network, and the copy of the authoritative electronic record may be printed and stored at the remote location. Software at the remote location provides for receiving the version of the copy of the authoritative electronic record and digitally signing the authoritative electronic record. A message digest is created at the remote location by ~~combining~~ retrieving a ~~partial~~ partially completed message digest from the repository ~~with the remaining message digest information from~~ and completing the computation of the message digest over the copy of the authoritative electronic record and some appended identifying information ~~of the new digital signature, at the remote location~~. The digital signature on the authoritative electronic record at the repository is then created at the remote location using this message digest just created at the

remote location and the private key. The person then transmits the new digital signature and identifying information of the new digital signature back to the secure environment where the repository provides for validating the digital signature of the authoritative electronic record signed at the remote location against the existing authoritative electronic record stored at the repository through standard digital signature validation techniques.--

Please replace paragraph 0039 (beginning at page 10) with the following rewritten paragraph:

--A key point of the present invention is that it leaves only one ~~copy~~ instance of a unique authoritative electronic record, which resides in the secure repository. The present invention does not prevent the ability to make copies of the record, but it does ensure that copies made are easily distinguished as copies.--

Please replace paragraph 0040 (beginning at page 10) with the following rewritten paragraph:

--Another key point of the present invention ~~to~~ is that it allows a person to electronically sign an electronic record at a remote location without compromising the uniqueness of a corresponding authoritative electronic record. --

Please replace paragraph 0054 (beginning at page 11) with the following rewritten paragraph:

--FIG. 2 shows the initial operation of the present system. Record 6 is sent from a remote location to the repository 5. Record 6 is receipted within repository 5 by prepending receipt 7 to the beginning of record 6 and appending receipt 8 to the end of record 6. In an exemplary embodiment, receipt 7 is the repository's digital signature of the combination of both record 6 and some identifying information. Receipt 8 includes the identifying information and a ~~is an un-encrypted~~ message digest of the combination of both record 6 and the identifying information. Identifying information can include a time-stamp and the originator of the record. All information that has been encrypted, including actual digital signatures in FIGS. 2-4, is shown in double-framed format.--

Please replace paragraph 0058 (beginning at page 13) with the following rewritten paragraph:

--The interim chaining values are computed in two steps. The first step involves padding to a known bit value the existing beginning information with the necessary bits to make the bit length of the beginning information an integer multiple of ~~the~~ a certain bit length ~~in each~~ required for the given message digest algorithm. The same message digest algorithm will also be employed to complete the message digest used in the desired digital signature at the remote location. The second step involves inputting the now padded bit stream of the beginning information into the message digest algorithm to produce the interim chaining values. This process of creating the chaining values is called "interim" because the final hashing of the entire message is not completed at the repository 5. Rather, this final hashing will be completed at the remote location.--

Please replace paragraph 0060 (beginning at page 13) with the following rewritten paragraph:

--The person then uses his private key to create a digital signature with the complete message digest, thereby signing the receipted record 6-8 and producing digital signature 11. The digital signature 11 may include encoding information. In this embodiment, a small hardware token or smart card provides the private key used by the person for ~~encryption~~ digitally signing. Alternatively, in some circumstances, a software-based private key may be used. Digital signature 11 along with any identifying information is then transmitted to repository 5 where it is validated with the public key and a recomputed message digest of receipted record 6-8 (including any new identifying information). A positive match validates the digital signature 11 and establishes that:--

Please replace paragraph 0067 (beginning at page 14) with the following rewritten paragraph:

--Continuing in FIG. 3, after validation of the digital signature 11, the process of revising the authoritative record begins by prepending digital signature 11 to the beginning of the authoritative record 6-8, and appending signature information 12 to the end of authoritative record 6-8. In this embodiment, signature information 12 comprises any identifying information included in the message digest for the digital signature~~,~~ and the message digest used to produce the digital signature~~, and a timestamp~~. Of course, more or

less information can be included or excluded from the signature information 12. The operation of revising the authoritative record is continued in FIG. 4.--

Please replace paragraph 0068 (beginning at page 14) with the following rewritten paragraph:

--Referring to FIG. 4, digital signature 11 has been prepended to, and signature information 12 has been appended to, the authoritative record 6-8, thus increasing the amount of beginning and ending information, respectively. The repository 5 can then receipt the signed record 6-8 and 11-12, by prepending a repository-created digital signature, which serves as ~~digitally signed~~ receipt 13, to the signed record, and appending identifying receipt information 14 to~~,~~ the signed record. The receipted signed record 6-8 and 11-14 is now the "revised authoritative record" replacing the earlier authoritative record 6-8. When further requests are received for a copy of the record, the revised authoritative record 6-8 and 11-14 will be used to generate the copies following the procedure outlined in the discussion of FIG. 2. As shown in FIG. 4, the copy of the revised authoritative record will consist of record 6 and all ending information; appended information 8, 12, and 14, in this case. The process of transmitting a copy of the authoritative record over the partially un-trusted network 4 is then repeated, wherein the transmission is normally encrypted with a symmetric key to produce encrypted copy 15 which the requestor decrypts using the symmetric key at a remote location.--

Please replace paragraph 0069 (beginning at page 15) with the following rewritten paragraph:

--FIG. 5 is a flow chart for the overall operation of the present system. In step S500, an electronic record is sent to the repository 5 from a remote location. In step S502, a unique authoritative record is created and stored within repository 5. When a person at a remote location wants to sign the authoritative record, a copy of the authoritative record is made that is distinctly different from, but perceptively the same as, the authoritative record. The distinctly different copy and a partial message digest for the beginning information are sent to the person, at step S504. The copy of the authoritative record and the partial message digest can, of course, be sent in two separate steps. In step S506, the message digest is completed at the remote location using the copy of the authoritative record and identifying information as

input, and the remote location uses a private key and the completed message digest to create the digital signature. The digital signature and identifying information is then transmitted to the repository 5 where ~~it~~ the digital signature is validated and upon affirmative validation, the authoritative record is revised with the digital signature and other information, step S508.--

Please replace paragraph 0070 (beginning at page 15) with the following rewritten paragraph:

--FIGS. 6A-6D provide a detailed flow chart of exemplary embodiments for carrying out the method discussed in association with FIG. 5. In FIG. 6A, an exemplary embodiment for receipting a record in repository 5 and generating the initial authoritative record is illustrated. In step S600 the record is received in the present repository, which may also be referred to as a trusted repository. In step S602 a time stamp~~, which may include other identifying information,~~ is completed for and appended to the record as part of some identifying information. The phrase "receipted record", as it pertains to Fig. 6A, refers to any record received by the secure environment that has been time-stamped in this manner. Step ~~S604~~ S602 is the first step in generating the initial authoritative record.--

Please replace paragraph 0071 (beginning at page 16) with the following rewritten paragraph:

--The authoritative record is important because the authoritative record is the record that must remain unique, to ensure legal enforceability under current electronic transaction laws. In step S604, a single message digest is generated of the record and identifying information, which includes the time stamp. In step S606 a digital signature, which serves as a receipt, is created using the message digest and a private key ~~the message digest is digitally signed to create a receipt~~, and ~~the~~ this receipt is then prepended to the beginning of the record. The prepended receipt and any later prepended information is referred to as "beginning information". In step S608 ~~identifying~~ information related to the receipt (such as, for example, the message digest corresponding to the receipt) is appended to the end of the record. ~~The appended identifying information identifies the receipt as the repository's signature and includes other information.~~ The appended information, including the time stamp and other previously appended information, and any later appended information, is referred to as "ending information". The record together with beginning information and

ending information make up the "authoritative record" and at step S610 the authoritative record is stored in the repository 5.--

Please replace paragraph 0073 (beginning at page 17) with the following rewritten paragraph:

--FIG. 6C details the signing operation by a person at a remote location. Prior to signing the authoritative record, portions of the record maintenance software have been loaded on the signatory's computer or workstation. At step S620 the person decides to sign the authoritative record. In order to sign the record the person must first create a message digest of the authoritative record. Since the person at the remote location does not have the beginning information, which was retained in the repository 5, the software requests additional information from the repository 5. At step S622, the repository 5 in response generates a partial message digest using the beginning information as input and transmits the partial message digest to the remote location. The partial message digest comprises interim chaining values of the beginning information (which additionally includes any required padding) and the length of the beginning information (along with any padding). If by chance a second person has signed the same authoritative record, between the time the first person requested the record at step S612 and decided to sign the record at step S620, then the system takes appropriate steps to make sure the first person receives and signs a revised authoritative record. Primarily, the first person is notified of the new signature and is sent a revised copy and a revised partial message digest. The person then continues with the normal signing process described below.--

Please replace paragraph 0074 (beginning at page 17) with the following rewritten paragraph:

--At step S624 the person receives the partial message digest. At step S626, the remote location uses the interim chaining values of the partial message digest to reseed the message digest algorithm and complete a message digest for the authoritative record that was begun in the repository 5 possibly appending user-added information to the end of the record before completing the message digest. In step S628 the resulting message digest~~, and any user added information,~~ is then ~~digitally signed~~ used along with the person's private key~~, thereby generating~~ to generate a digital signature. In step S630 the digital signature, along with any user added information, is transmitted to the repository 5. And in step S632 the signature is

validated in the repository 5. The first step in validation is computing a single message digest of both the authoritative record stored in the repository 5 and any additional identifying information added by the signer ~~on his copy of the message digest~~.--

Please replace paragraph 0075 (beginning at page 17) with the following rewritten paragraph:

--Using this ~~authoritative record~~ computed message digest, the uploaded digital signature, and the corresponding public key, the digital signature is validated by either using a validating algorithm in the case of a DSA-type digital signature or message digest comparison in the case of a RSA-type digital signature. A validation or perfect match indicates a valid digital signature.--

Please replace paragraph 0076 (beginning at page 18) with the following rewritten paragraph:

--FIG. 6D illustrates the steps for revising the authoritative record once a digital signature has been validated. A decision is made in step S634. If the digital signature was not validated in step S632 then the process must restart at step S614 where a new copy will be made and sent to the remote location. If, at step S634, the signature was determined to be valid, then we proceed to step S638 where authorization is given to create a revised authoritative record. Generating a revised authoritative record, in a preferred embodiment, involves prepending the digital signature to the beginning of the current authoritative record and appending signature information to the end of the current authoritative record. In step S640 the digital signature is prepended to the beginning of the authoritative record. It should be understood that the digital signature may have additional information attached thereto prior to prepending. In step S642 signature information, which includes the message digest used to create the digital signature at the remote location, and which may also include additional user-added information, is appended to the end of the authoritative record. In step S644 a receipt of the partially revised authoritative record is prepended to the beginning of the partially revised authoritative record, i.e., the beginning of the prepended digital signature. And in step S646 identifying information for the receipt of the partially revised authoritative record is appended to the end of the partially revised authoritative record, i.e., to the end of the signature information. This combination of the digital signature and repository receipt prepended to the "old" authoritative record and the signatory information and

identifying information appended to the "old" authoritative record is the "revised authoritative record". At step S648 the revised authoritative record is stored in ~~a~~ the repository 5. It should also be understood that previous artifact records, receipts, digital signatures, ~~and~~ identifying information, etc., may also be maintained separately in the repository 5.--